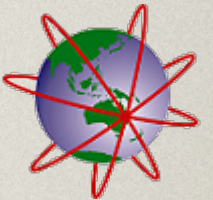


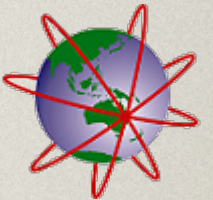


Securing the Web without site-specific passwords





F**k all of these
passwords, we can
do better than this!



solving the
password problem
on the web

problem #1:

passwords are **hard to secure**





Linked 

YAHOO![®]





Linked in

YAHOO!®

STEAM™

livingsocial®

IEEE

Linked 

YAHOO!®

 STEAM™


livingsocial®

 IEEE

eHarmony®

Linked 

YAHOO!®

 STEAM™


livingsocial®

 IEEE

eHarmony®

rockyou

Linked 

YAHOO!®

 STEAM™

 livingsocial®

 IEEE

eHarmony®

rockyou

SONY
PICTURES

Linked 

YAHOO!®

 STEAM™

 livingsocial®

 IEEE

eHarmony®

rockyou

SONY
PICTURES

last.fm

Linked 

YAHOO!®

 STEAM™


livingsocial®

 IEEE

eHarmony®

rockyou

SONY
PICTURES

last.fm

 EVERNOTE®



bcrypt / scrypt / pbkdf2

 bcrypt / scrypt / pbkdf2

 per-user salt



bcrypt / scrypt / pbkdf2



per-user salt



site secret

 bcrypt / scrypt / pbkdf2

 per-user salt

 site secret

 password & lockout policies



bcrypt / scrypt / pbkdf2



per-user salt



site secret



password & lockout policies



secure recovery



bcrypt / scrypt / pbkdf2



per user salt



site secret



password & logout policies



secure recovery

2013 password guidelines

passwords are hard to secure
they are a **liability**

```
ALTER TABLE user  
DROP COLUMN password;
```

problem #2:

passwords are **hard to remember**

users have **two** strategies

1. pick an easy password



LastPass *****

Passwords and forms

- ☐ Enable Auto-fill to fill in web forms in a single click. [Manage Auto-fill settings](#)
- ☒ Offer to save passwords I enter on the web. [Manage saved passwords](#)

Passwords

- ☒ Remember passwords for sites
- ☐ Use a master password

THE PERSONAL
**internet
address &
password
logbook**

*Keep favorite website addresses,
usernames, and passwords in
one easy, convenient place!*



PETER PAUPER PRESS

2. reuse your password

negative externality:

sites that don't care about security
impose **a cost on more important sites**

passwords are hard to remember
they need to be **reset**

Reset Your Password

Enter your email address below and we'll send you a link with instructions.

Submit

Forgot password

Email

wtf@lloyd.io

Submit

Lost password

Follow these simple steps to reset your account:

1. Enter your **WordPress.com** username or email address
2. Wait for your recovery details to be sent
3. Follow instructions and be re-united with your **WordPress.com** account

Want more help? We have a full [guide to resetting your password](#).

Username or E-mail:

[Need More Help?](#)

Get New Password

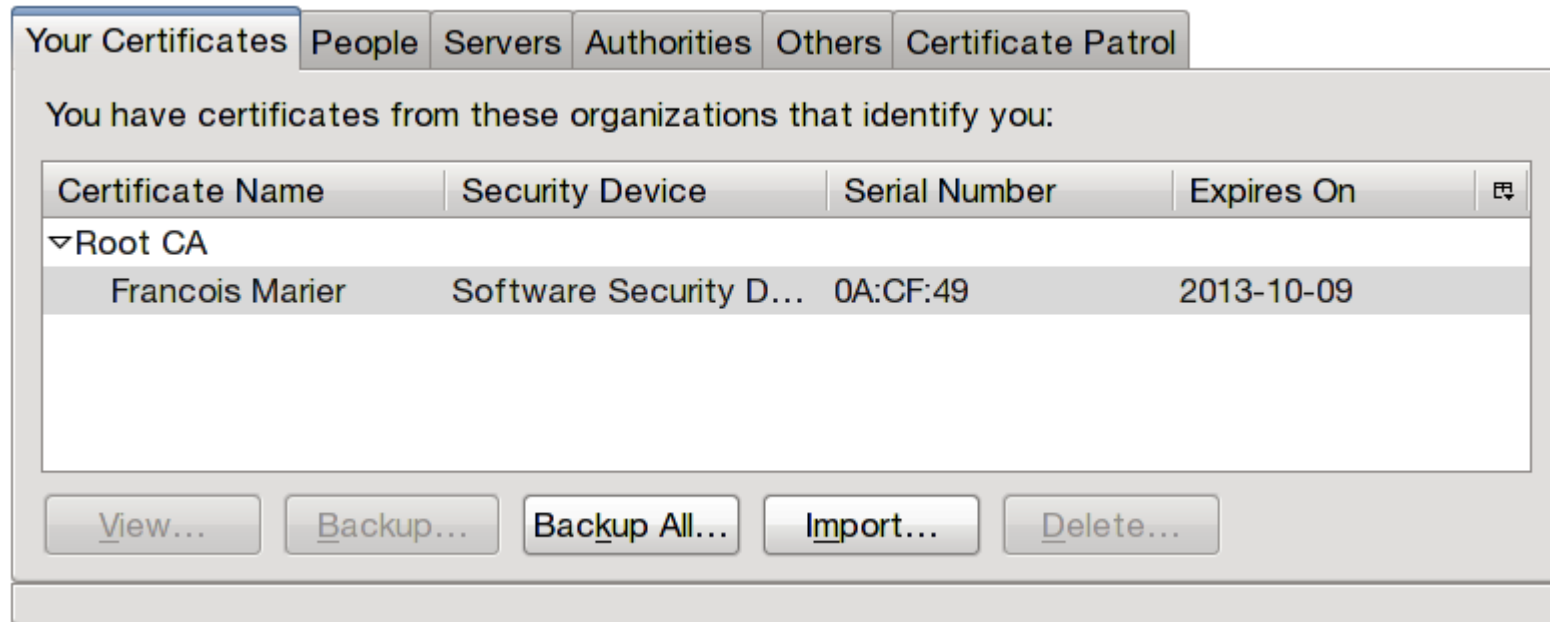
control
email
account

=

control
all
accounts

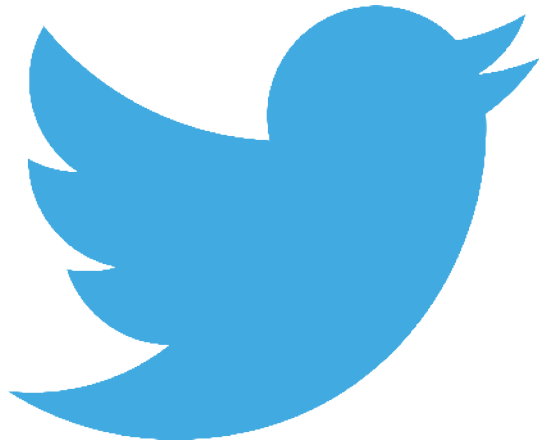
existing login solutions

client certificates





centralised authorities



existing login systems
are not good enough

ideal web-wide identity system

ideal web-wide identity system

- decentralised

ideal web-wide identity system

- decentralised
- simple

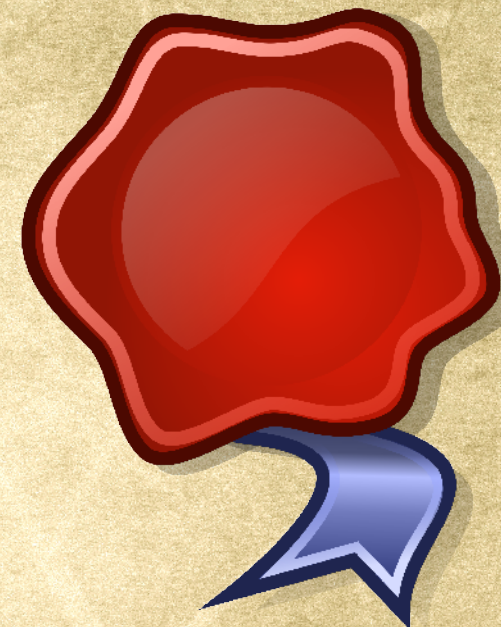
ideal web-wide identity system

- decentralised
- simple
- cross-browser



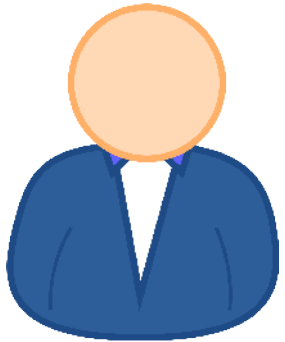
- decentralised
- simple
- cross-browser

how does it work?

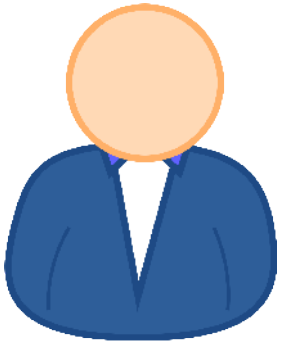


fmarier@gmail.com

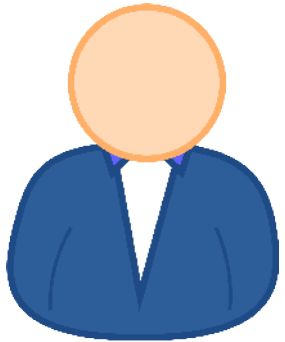
getting a proof of email ownership



authenticate?



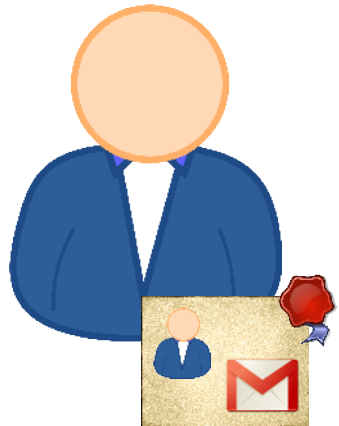
authenticate?



public key



authenticate?

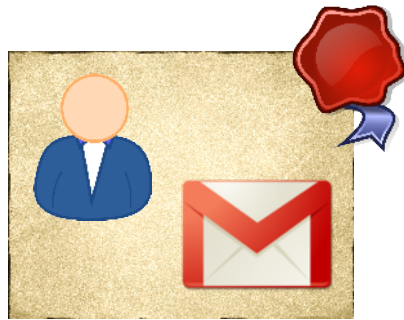


public key



signed public key

you have a **signed statement** from your provider that you **own** your email address

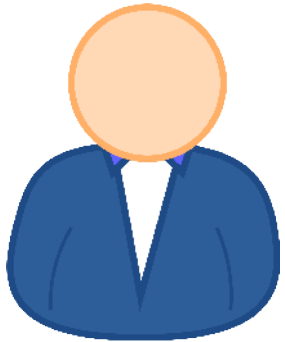




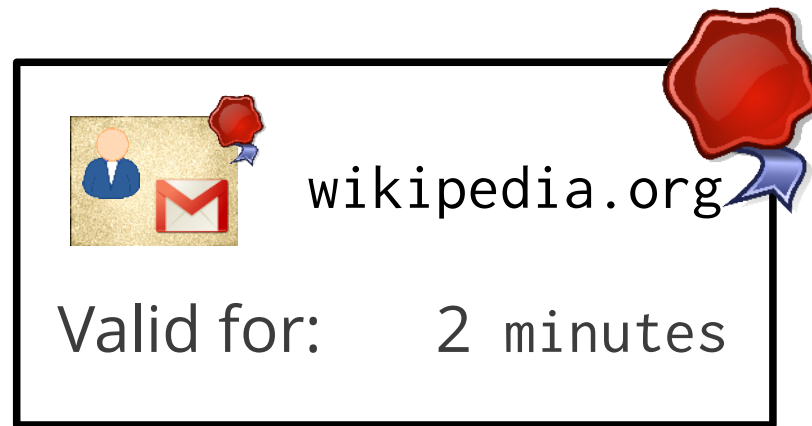
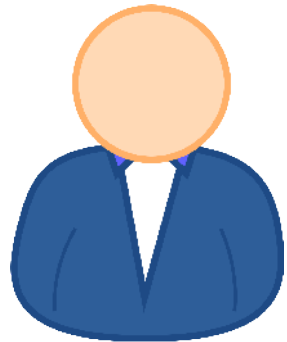
PASSPORT



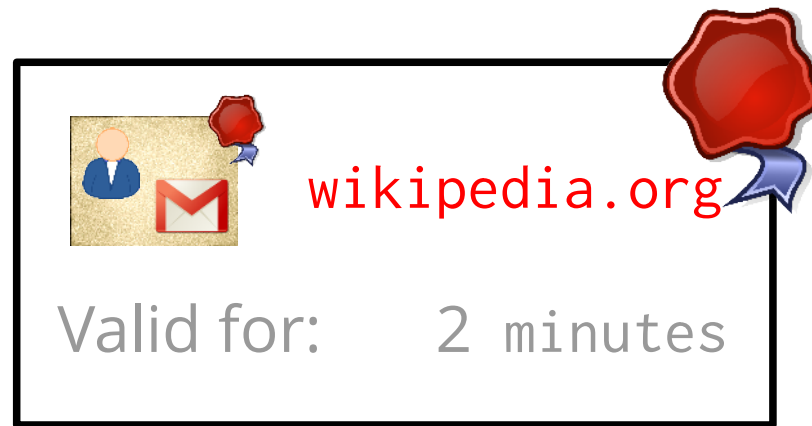
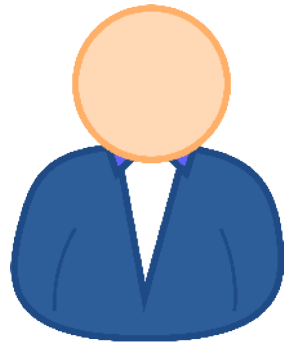
logging into a 3rd party site



assertion

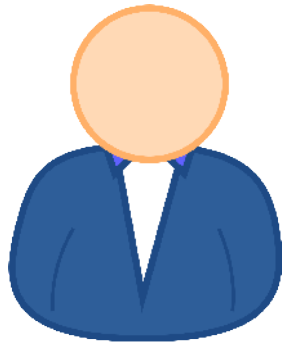


assertion



check audience

assertion

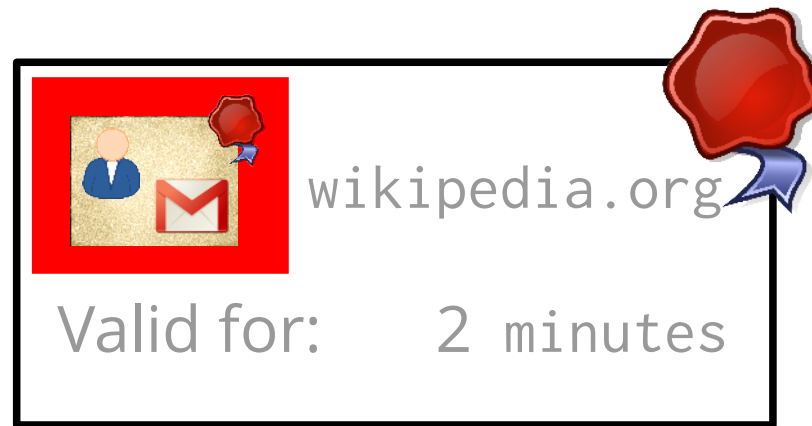
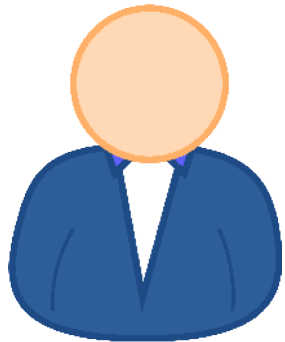


check audience



check expiry

assertion



check audience

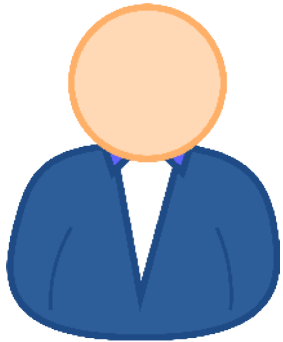


check expiry

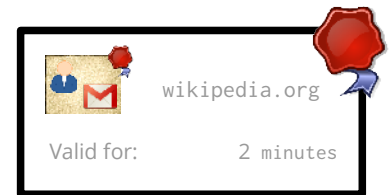
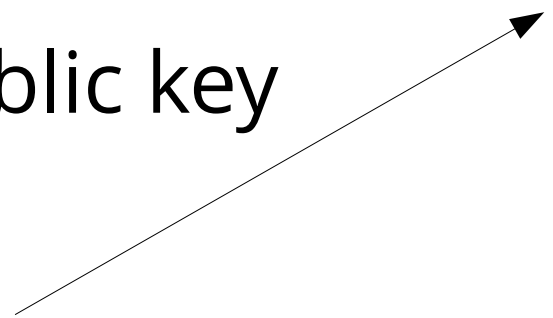


check signature

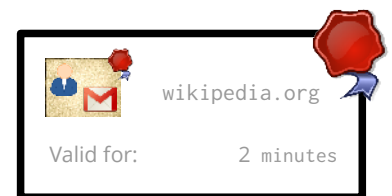
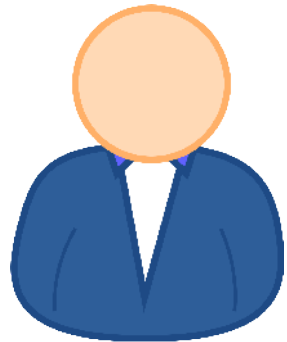
assertion

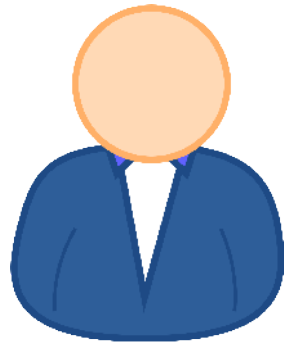


public key



assertion





assertion



session cookie





demo #1:

<http://crossword.thetimes.co.uk/>

fmarieretest@eyedee.me

Persona is already a
decentralised system

decentralisation matters for:

decentralisation matters for:

- choice

decentralisation matters for:

- choice
- security

decentralisation matters for:

- choice
- security
- innovation

SMS with PIN codes

Send My PIN.org

A [Mozilla Persona](#) Identity Provider

sendmypin.org is an experimental Mozilla Persona Identity Provider that allows you to sign in to sites using their SMS enabled phone.

To give sendmypin.org a try, visit your favorite Persona enabled site and sign in using <your_phone_number_with_country_code>@your_email_address.

A Friday Hack by [Shane Tomlinson](#) Source code on [GitHub](#)

SMS with PIN codes

Jabber / XMPP



SMS with PIN codes

Jabber / XMPP

Yubikeys



SMS with PIN codes

Jabber / XMPP

Yubikeys

LDAP accounts



A screenshot of a 'Sign In' dialog box for Mozilla Corporation. The dialog has a white background with a light gray border. At the top, the 'mozilla' logo is in a large, bold, red font, with 'CORPORATION' in a smaller, red, all-caps font below it. Underneath the logo, the text 'Sign In' is in a black serif font, followed by the instruction 'Please use your LDAP password' in a smaller black sans-serif font. There are two input fields: the first is labeled 'Email' in a bold black sans-serif font, and the second is labeled 'Password' in a bold black sans-serif font. Both labels are to the left of their respective white input boxes with thin gray borders. At the bottom of the dialog, there are two buttons: 'Sign in' and 'Cancel', both in a gray sans-serif font with a slight 3D effect.

mozilla
CORPORATION

Sign In
Please use your LDAP password

Email

Password

Sign in Cancel

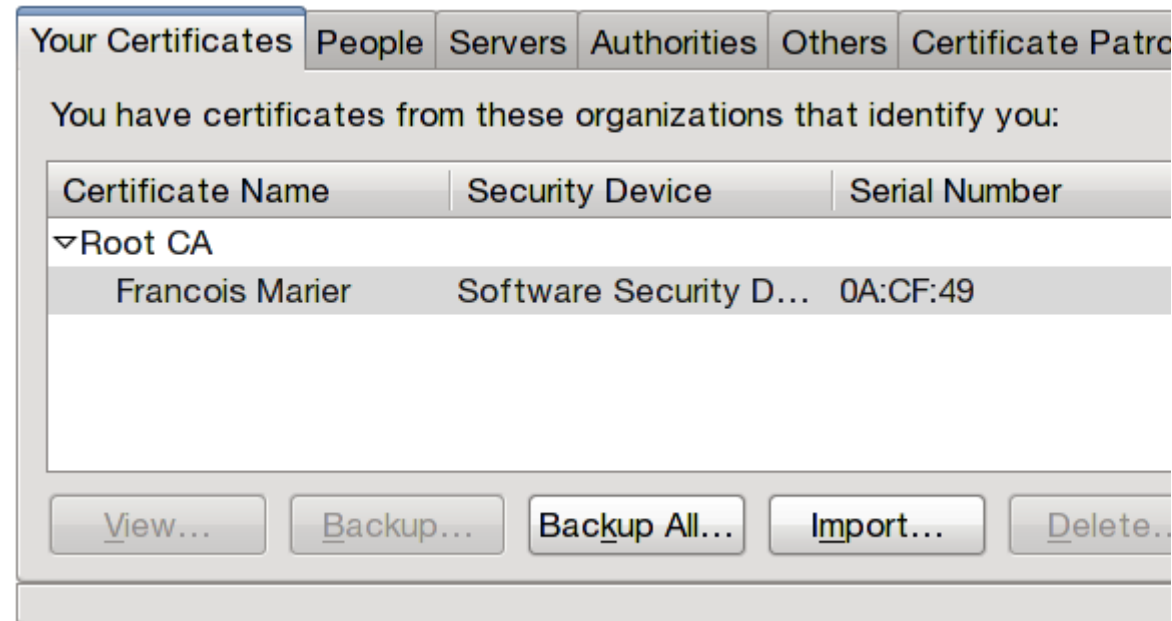
SMS with PIN codes

Jabber / XMPP

Yubikeys

LDAP accounts

Client certificates



SMS with PIN codes

Jabber / XMPP

Yubikeys

LDAP accounts

Client certificates

Password-wrapped secret key

```
{  
  "public-key": {  
    "algorithm":  
      "RS",  
    "n": "685484565272...",  
    "e": "65537"  
  },  
  "encrypted-private-key": {  
    "iv": "tmg7gztUQT...",  
    "salt": "JMtGw1F5UWY",  
    "ct": "8Dd0jD1IA1..."  
  },  
  "authentication": "...",  
  "provisioning": "..."  
}
```

decentralisation enables
innovation

decentralisation is the answer, but it's not
a **product adoption strategy**

we can't wait for **all domains**
to adopt Persona

we can't wait for **all domains**
to adopt Persona

solution: a temporary
centralised **fallback**



demo #2:

<http://sloblog.io/>

fmariertest@gmail.com

Persona already works
with **all email domains**

identity bridging



demo #3:

<http://www.reasonwell.com/>

fmariertest@yahoo.com

YAHOO![®]

YAHOO!

Gmail™

 Hotmail



Persona supports
all modern browsers



Persona is decentralised,
simple and cross-browser

it's simple for **users**, but is it also
simple for **developers**?

Add item

add

So what is all this then?

123done.org is a very simple to-do list application. Simply enter your to-do list item above and add it to your tasks. Click the tasks to mark them as done. Clicking an already finished task will remove it from the list.

Your task list is stored on the computer for you to use. If you want to sync 123done across devices, log in with Mozilla Persona.

123done is a project to show the power of Persona. Written by the identity folks at Mozilla.

```
<script src="https://login.persona.org/include.js">  
</script>  
</body></html>
```

```
navigator.id.watch({
```

```
});
```



```
navigator.id.watch({  
  loggedInUser: “francois@mozilla.com”,
```

```
});
```

```
navigator.id.watch({  
  loggedInUser: null,
```

```
});
```

```
navigator.id.watch({  
  loggedInUser: null,  
  onlogin: function (assertion) {
```

```
  },
```

```
});
```

```
navigator.id.watch({  
  loggedInUser: null,  
  onlogin: function (assertion) {  
  
  
  
  
  
  
  },  
  onlogout: function () {  
    window.location = '/logout';  
  }  
});
```



Add item

add

So what is all this then?

123done.org is a very simple to-do list application. Simply enter your to-do list item above and add it to your tasks. Click the tasks to mark them as done. Clicking an already finished task will remove it from the list.

Your task list is stored on the computer for you to use. If you want to sync 123done across devices, log in with Mozilla Persona.

123done is a project to show the power of Persona. Written by the identity folks at Mozilla.

```
navigator.id.request()
```


Add item

new item

add

 mozilla
Persona

☐ fmarier@mozilla.com

☐ francois@mozilla.com

By clicking sign in, you confirm that you accept this site's [Terms of Use](#) and [Privacy Policy](#).



123done

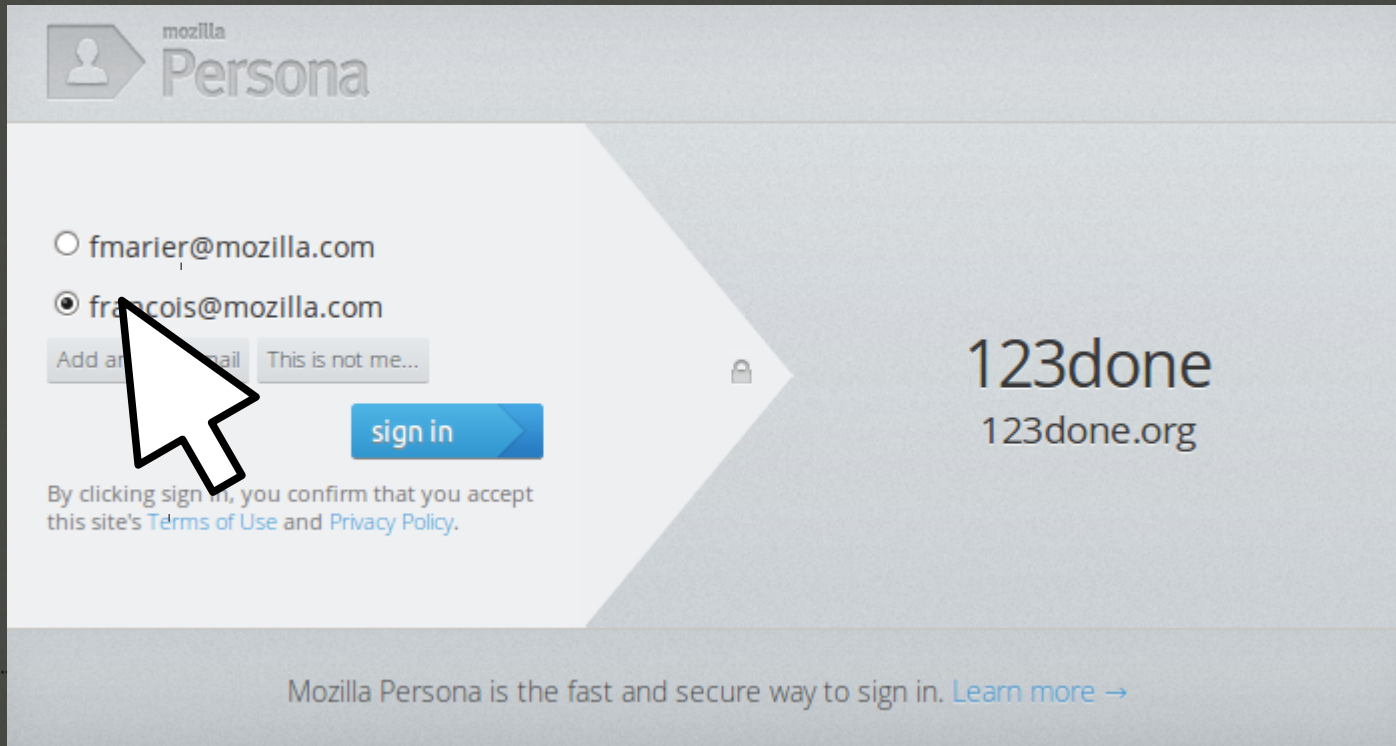
123done.org

Mozilla Persona is the fast and secure way to sign in. [Learn more →](#)

Add item

new item

add



The screenshot shows the Mozilla Persona sign-in interface for the 123done website. At the top left is the Mozilla Persona logo. Below it, two email addresses are listed with radio buttons: `fmarier@mozilla.com` and `francois@mozilla.com`. The second email is selected. Below the emails are two buttons: "Add another email" and "This is not me...". A large white mouse cursor arrow points towards the "sign in" button, which is a blue button with a right-pointing arrow. Below the "sign in" button, a line of text states: "By clicking sign in, you confirm that you accept this site's [Terms of Use](#) and [Privacy Policy](#)." To the right of the email selection area, there is a lock icon and the text "123done" and "123done.org". At the bottom of the page, a footer line reads: "Mozilla Persona is the fast and secure way to sign in. [Learn more](#) →".

mozilla
Persona

☐ fmarier@mozilla.com
☒ francois@mozilla.com

Add another email This is not me...

sign in

By clicking sign in, you confirm that you accept this site's [Terms of Use](#) and [Privacy Policy](#).

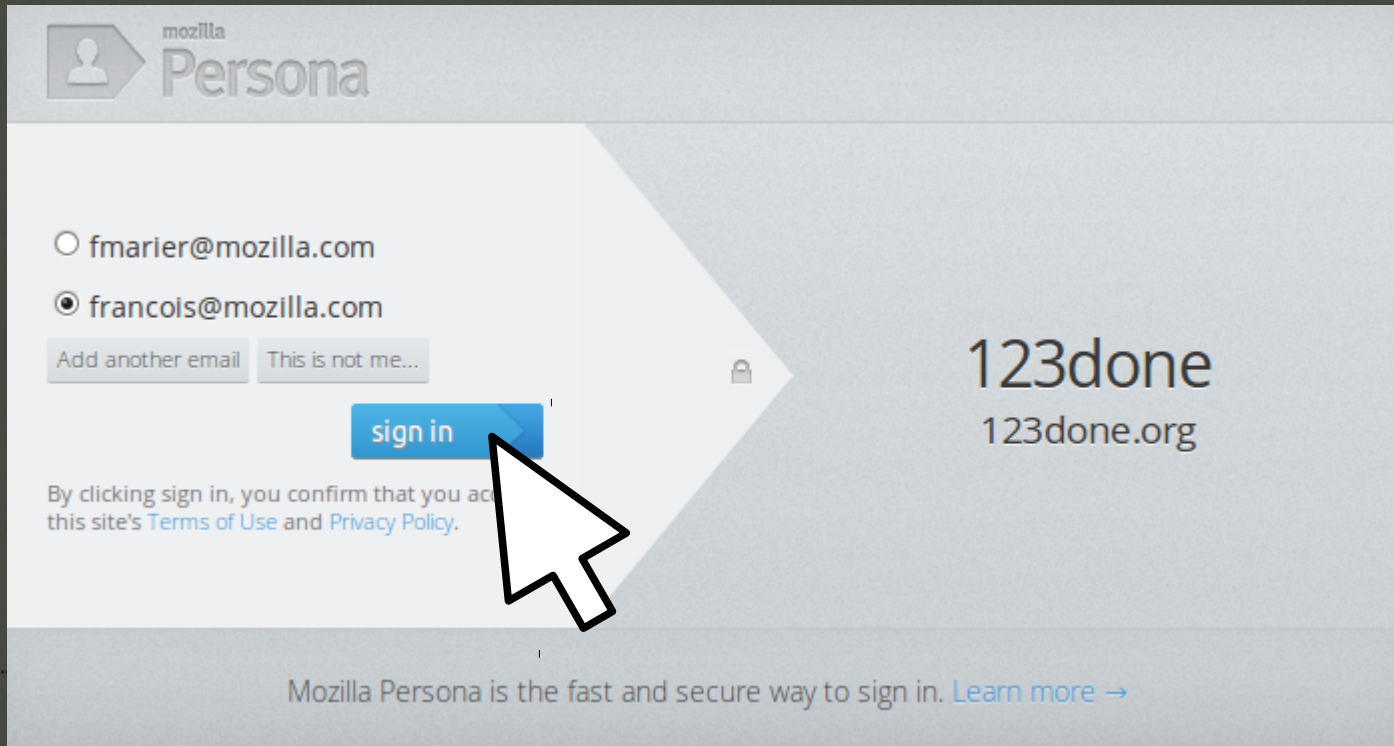
123done
123done.org

Mozilla Persona is the fast and secure way to sign in. [Learn more](#) →

Add item

new item

add



The screenshot shows the Mozilla Persona sign-in interface for the 123done website. At the top left is the Mozilla Persona logo. Below it, two email addresses are listed: `fmarier@mozilla.com` (unselected) and `francois@mozilla.com` (selected with a radio button). Below the emails are two buttons: "Add another email" and "This is not me...". A blue "sign in" button is positioned below the selected email, with a white mouse cursor pointing at it. To the right of the email selection area is a small lock icon. Further right, the text "123done" and "123done.org" is displayed. At the bottom, a footer message states: "Mozilla Persona is the fast and secure way to sign in. [Learn more →](#)".

mozilla
Persona

☐ fmarier@mozilla.com

☒ francois@mozilla.com

Add another email This is not me...

sign in

By clicking sign in, you confirm that you agree to this site's [Terms of Use](#) and [Privacy Policy](#).

123done
123done.org

Mozilla Persona is the fast and secure way to sign in. [Learn more →](#)

```
navigator.id.watch({  
  loggedInUser: null,  
  onlogin: function (assertion) {  
  
  
  
  
  
  
  },  
  onlogout: function () {  
    window.location = '/logout';  
  }  
});
```

```
navigator.id.watch({
  loggedInUser: null,
  onlogin: function (assertion) {
    $.post('/login',
      {assertion: assertion},
      function (data) {
        window.location = '/home';
      }
    );
  },
  onlogout: function () {
    window.location = '/logout';
  }
});
```

```
$ curl -d "
```

```
"
```

```
https://verifier.login.persona.org/verify
```

```
$ curl -d "assertion=<ASSERTION>&  
          audience=http://123done.org"  
https://verifier.login.persona.org/verify
```

```
{  
  status: "okay",  
  audience: "http://123done.org",  
  expires: 1344849682560,  
  email: "francois@mozilla.com",  
  issuer: "login.persona.org"  
}
```

```
{  
  status: "failed",  
  reason: "assertion has expired"  
}
```






✓ prepare slides
deliver presentation
profit from merch sales

Add item

add

So what is all this then?

123done.org is a very simple to-do list application. Simply enter your to-do list item above and add it to your tasks. Click the tasks to mark them as done. Clicking an already finished task will remove it from the list.

Your task list is stored on the computer for you to use. If you want to sync 123done across devices, log in with Mozilla Persona.



✓ prepare slides
deliver presentation
profit from merch sales

Add item

add

So what is all this then?

123done.org is a very simple to-do list application. Simply enter your to-do list item above and add it to your tasks. Click the tasks to mark them as done. Clicking an already finished task will remove it from the list.

Your task list is stored on the computer for you to use. If you want to sync 123done across devices, log in with Mozilla Persona.

```
navigator.id.logout()
```

```
navigator.id.watch({
  loggedInUser: null,
  onlogin: function (assertion) {
    $.post('/login',
      {assertion: assertion},
      function (data) {
        window.location = '/home';
      }
    );
  },
  onlogout: function () {
    window.location = '/logout';
  }
});
```


Add item

add

So what is all this then?

123done.org is a very simple to-do list application. Simply enter your to-do list item above and add it to your tasks. Click the tasks to mark them as done. Clicking an already finished task will remove it from the list.

Your task list is stored on the computer for you to use. If you want to sync 123done across devices, log in with Mozilla Persona.

123done is a project to show the power of Persona. Written by the identity folks at Mozilla.

1. load javascript library

1. load javascript library

2. setup login & logout callbacks

1. load javascript library
2. setup login & logout callbacks
3. add login and logout buttons

1. load javascript library
2. setup login & logout callbacks
3. add login and logout buttons
4. verify proof of ownership

you can add support for
Persona in four easy steps

one simple request

STOP

building a **new** site:
default to Persona



working on an **existing** site:
add support for Persona





we need
your help

to eliminate
site-specific
passwords

To learn more about Persona:

<https://login.persona.org/>

<http://identity.mozilla.com/>

https://developer.mozilla.org/docs/Persona/Why_Persona

https://developer.mozilla.org/docs/Persona/Quick_Setup

<https://github.com/mozilla/browserid-cookbook>

https://developer.mozilla.org/docs/Persona/Libraries_and_plugins

<http://123done.org/>

https://wiki.mozilla.org/Identity#Get_Involved

@fmarier

<http://fmarier.org>

identity provider API

`https://eyedee.me/.well-known/browserid`

identity provider API

`https://eyedee.me/.well-known/browserid:`

```
{  
  "public-key": {  
    "algorithm": "RS",  
    "n": "8606...",  
    "e": "65537"  
  },  
  "authentication": "/browserid/sign_in.html",  
  "provisioning": "/browserid/provision.html"  
}
```

identity provider API

`https://eyedee.me/.well-known/browserid:`

```
{  
  "public-key": {  
    "algorithm": "RS",  
    "n": "8606...",  
    "e": "65537"  
  },  
  "authentication": "/browserid/sign_in.html",  
  "provisioning": "/browserid/provision.html"  
}
```

identity provider API

`https://eyedee.me/.well-known/browserid:`

```
{  
  "public-key": {  
    "algorithm": "RS",  
    "n": "8606...",  
    "e": "65537"  
  },  
  "authentication": "/browserid/sign_in.html",  
  "provisioning": "/browserid/provision.html"  
}
```

identity provider API

`https://eyedee.me/.well-known/browserid:`

```
{  
  "public-key": {  
    "algorithm": "RS",  
    "n": "8606...",  
    "e": "65537"  
  },  
  "authentication": "/browserid/sign_in.html",  
  "provisioning": "/browserid/provision.html"  
}
```

identity provider API

1. check for your /.well-known/browserid

identity provider API

1. check for your `/.well-known/browserid`
2. try the provisioning endpoint

identity provider API

1. check for your `/.well-known/browserid`
2. try the provisioning endpoint
3. show the authentication page

identity provider API

1. check for your `/.well-known/browserid`
2. try the provisioning endpoint
3. show the authentication page
4. call the provisioning endpoint again

Photo credits:

Top 500 passwords: <http://xato.net/passwords/more-top-worst-passwords/>

Parchment: <https://secure.flickr.com/photos/27613359@N03/6750396225/>

Cookie on tray: <https://secure.flickr.com/photos/jamisonjudd/4810986199/>

Uncle Sam: <https://secure.flickr.com/photos/donkeyhotey/5666065982/>

Australian passport: <https://secure.flickr.com/photos/digallagher/5453987637/>

Stop sign: <https://secure.flickr.com/photos/artbystevejohnson/6673406227/>



© 2013 François Marier <francois@mozilla.com>

This work is licensed under a

[Creative Commons Attribution-ShareAlike 3.0 New Zealand](https://creativecommons.org/licenses/by-sa/3.0/nz/) License.